**1 CÔNG NGHỆ CHUỖI KHỐI** **A triangle with words in it

Description automatically generated**

**1. CƠ SỞ DỮ LIỆU TẬP TRUNG VÀ PHI TẬP TRUNG**

**Hệ thống thông tin**

Công nghệ thông tin (*Information Technology*), là áp dụng Khoa học máy tính (*Computer Science*) giải quyết các bài toán trong thực tế theo nghĩa xem các chương trình máy tính (*computer programs*) như hệ thống biến đổi các thông tin hay dữ liệu đầu vào (*data input*) thành các thông tin hay dữ liệu đầu ra (*data output*) dựa trên các thuật toán (algorithm) đã được lập trình (*programming*). Theo đó,

Thông tin được xem là thành phần trọng tâm của các hệ thống máy tính.

Một số chương trình máy tính, đặc biệt các hệ thống hỗ trợ quản lý, gọi chung là hệ thống thông tin (*information systems*), dữ liệu có thể được xem như ‘*trái tim*’ của hệ thống trong khi chương trình là cài đặt mô phỏng các quy trình nghiệp vụ (*business process*). Trong các hệ thống thông tin này, dữ liệu được tổ chức và được tập hợp thành các cơ sở dữ liệu (*database*), là tập hợp các dữ liệu thể hiện (*instance*) của thực thể (*entity*) cần quản lý.

**Cơ sở dữ liệu**

Về hình thức, Cơ Sở Dữ Liệu, viết tắt là **CSDL** hay **DB**, là một tập hợp các dữ liệu có liên quan đến nhau, được tổ chức và thường được lưu trữ, truy cập điện tử từ hệ thống máy tính. Cấu trúc thực thể cũng như sự quan hệ giữa các thực thể có thể được mô hình hóa (*data modelling*) để có thể lưu trữ và xử lý hiệu quả nhất có thể. Mô hình thực thể-kết hợp (**ERM** – *Entity Relationship Model*)[[1]](#footnote-1) là mô hình ý niệm (*concept model*) đang được sử dụng phổ biến cho quá trình thiết kế mô hình dữ liệu. Trong tài liệu này, để đơn giản, ta sẽ giới hạn mô hình chỉ gồm một thực thể trong một lược đồ quan hệ (*relation scheme*). Về mặt ý niệm, mỗi thực thể được quản lý qua các thuộc tính (*attributes*) có quan hệ nội tại với nhau trong cùng một thực thể. Về mặt vật lý, mỗi lược đồ quan hệ, gọi tắt là một quan hệ (**R** – *Relation*), được cài đặt như một bảng 2-chiều (*table*) và được lưu trữ trong một tập tin (*file*). Lưu trữ (*storing*) và truy xuất dữ liệu trong cơ sở dưc liệu, gọi chung là truy vấn (*querry*) được hỗ trợ bởi các hệ quản trị cơ sở dữ liệu (**DBMS** – *Data Base Management Systems*).

**Hệ quản trị CSDL**

Hệ quản trị cơ sở dữ liệu – **DBMS**, là (hệ thống) phần mềm được dùng để lưu trữ (*storing*), truy xuất (*access*) và chạy các truy vấn (*query*) trên CSDL. DBMS có thể xem như giao diện (*interface*) giữa người dùng cuối và cơ sở dữ liệu, cho phép người dùng tạo (*create*), đọc (*read*), cập nhật (*edit*) và xóa (*delete*) dữ liệu trong cơ sở dữ liệu. DBMS có thể được phân loại theo các tiêu chí khác nhau như mô hình dữ liệu, phân phối cơ sở dữ liệu hoặc số lượng người dùng. Các DBMS được sử dụng rộng rãi nhất là quan hệ, phân tán, phân cấp, hướng đối tượng và mạng. DB cũng như DBMS có thể được lưu trữ và xử lý tập trung (*centralization*) hay không tập trung (*non-centrolization*).

**CSDL tập trung và phân tán**

Cơ sở dữ liệu tập trung (**CDB** – *Centralized Data Base*) là cơ sở dữ liệu được định vị, lưu trữ và ***duy trì ở một vị trí duy nhất***. Vị trí này thường là máy tính trung tâm hoặc hệ thống cơ sở dữ liệu. Trong hầu hết các trường hợp, cơ sở dữ liệu tập trung sẽ được sử dụng bởi một cơ quan hay một tổ chức. Người dùng truy cập cơ sở dữ liệu tập trung thông qua mạng máy tính sau khi đã được cấp quyền truy cập vào hệ thống trung tâm, để tìm kiếm (*search*) hay duy trì (*maintain*) cơ sở dữ liệu đó.

Cơ sở dữ liệu phân tán (**DDB** – *Distributed Data Base*) là một loại cơ sở dữ liệu bao gồm nhiều cơ sở dữ liệu được kết nối với nhau và trải rộng trên các vị trí vật lý khác nhau. Dữ liệu được lưu trữ ở nhiều vị trí vật lý khác nhau có thể được quản lý độc lập với các vị trí vật lý khác.

Cụm từ *duy trì ở một vị trí duy nhất* trong khái niệm **CDB** hàm ý rằng ngay cả CSDL được lưu trữ phân tán ở nhiều vị trí vật lý hay địa lý khác nhau thì việc ***duy trì hay rộng hơn là giám sát vẫn được thực hiện ở một vị trí hay một người có quyền cao nhất***. Theo đó, ta vẫn có thể xem một DDB là CDB khi việc duy trì tập trung trong ‘một’ người. Ngược lại, ta gọi là CSDL phi-tập trung.

**CSDL phi-tập trung**

Cơ sở dữ liệu phi-tập trung (*Decentralized Data Base*), chính xác phải gọi là dữ liệu phi tập trung (*decentralized data*) là dữ liệu được tạo (*create*), lưu trữ (*storing*) và truy xuất (*access*) một cách độc lập từ nhiều vị trí khác nhau và không bị giám sát bởi bất kỳ tổ chức hay cá nhân nào.

Như vậy, CSDL phi-trập trung là cả lưu trữ lẫn xử lý phân tán. Điều này dẫn đến những thách thức trong việc duy trì CSDL chung, khi dữ liệu được phát triển thành CSDL – **Decentralized Database**.

**CSDL tập trung hay CSDL phi-tập trung?**

Cả CSDL tập trung lẫn phi-tập trung đều có những ưu thế và bất lợi riêng của chúng. Câu hỏi tự nhiên đặt ra là chọn CSDL nào: tập trung hay phi-tập trung?

Để trả lời, hãy xem hình vẽ minh họa về 2 tiêu chí quan trọng khi xem xét xây dựng một hệ thống thông tin: (**i**) hiệu năng (truy vấn) và (**ii**) bảo mật (security). Trước hết, cần lưu ý CSDL được tạo lập cho mục đích tìm kiếm là chính. Các thao tác khác như thêm (insert/append/add), xóa (delete/remove), hay cập nhật (edit) CSDL có thể không đòi hỏi phải xử lý cấp bách.

***Về tiêu chí (i): hiệu năng***. Do CSDL tập trung được lưu trữ và xử lý tại một điểm nên hiệu năng tìm kiếm cũng như duy trì CSDL là dễ dàng và hiệu quả. Truy vấn với CSDL tập trung đảm bảo tiêu chí hiệu năng. Ngược lại, với CSDL phi-tập trung, do dữ liệu được lưu trữ tại nhiều điểm khác nhau, CSDL chung chỉ là ý niệm với các thể hiện nằm ở các vị trí (vật lý cũng như địa lý) khác nhau nên việc đồng bộ (*synchronize*) để duy trì cho CSDL nhất quán là thách thức cho tiêu chí hiệu năng.

***Về tiêu chí (ii): bảo mật dữ liệu.*** Do tính tập, CSDL tập chỉ có một điểm tấn công vì thế dữ liệu không thực sự an toàn-bảo mật, đặc biệt, người có quyền cao nhất (*admin*) có toàn quyền và có thể làm sai lệch dữ liệu. Ngược lại, CSDL phi-tập trung, để tấn công, kẻ tấn công phải thay đổi được dữ liệu ở mọi điểm lưu trữ, mà sẽ bất khả thi nếu số điểm lưu trữ đủ nhiều.

|  |  |
| --- | --- |
| **Centralized Database** | **Decentralized Database** |
|  |  |

Tóm lại, việc chọn CSDL tập trung hay phi-tập trung cần phải được xem xét cẩn thận và tùy thuộc ứng dụng của hệ CSDL cần.

**CÔNG NGHỆ SỔ CÁI PHI TẬP TRUNG**

**Sổ cái.**

Thu nhỏ lại hoạt động của xã hội như những giao dịch (*transaction*) như trao đổi, vay mượn, buôn bán,… trực tiếp giữa các cá nhân trong công đồng với nhau. Để đảm bảo có vay thì phải trả, có bán thì mới mua,… các hoạt động cần có người làm chứng, nói cách khác, mọi giao dịch cần minh bạch, không có gì khuất tất. Mô hình giao dịch đơn giản này có thể được triển khai với khái niệm sổ-cái (*ledger*). Theo đó, ta hình dung, giữa làng đặt một sổ cái mà mọi người đều có thể đọc và gi lên đó công khai. Trong làng, ai vay của ai hay ai trả ai cái gì đều tự nguyện ghi lên sổ cái đó. Mọi tẩy xóa là không chấp nhận. Hình ảnh sổ cái công cộng (*public ledger*) với các giao dịch công khai như hình dưới, cho ta ý niệm ban đầu về việc vận hành ổn định xã hội một cách minh bạch và công khai. Chẳng hạn, sổ cái ghi

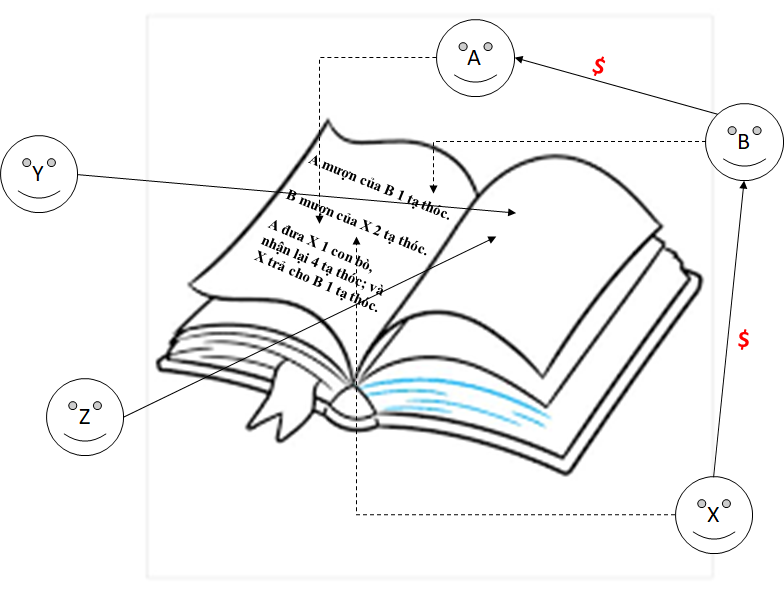
- “A mượn của B 1 tạ thóc.”

- “B mượn của X 2 tạ thóc.”

- “A đưa X 1 con bò, nhận lại 4 tạ thóc; và X trả cho B 1 tạ thóc.”

- …

Bằng cách quy đổi mọi thứ về một thứ ta gọi là “tiền tệ”, ký hiệu $, ta có mô hình kinh tế tiền tệ đơn giản như hình vẽ.



**Sổ cái phi tập trung**

Để đảm bảo sổ cái không bị phá hủy, vì một lý do nào đó như “chúa chổm” có thể hủy sổ cái để từ đó không còn bằng chứng nào chứng ninh hắn nợi-chúa-chổm. Vấn đề này có thể giải được bằng cách “phi tập trung sổ cái – **Decentralized Ledger**”, theo đó, sổ cái sẽ được giao cho n người giữ, mỗi người tự sao chép và cập nhật sổ cái mỗi khi có một giao dịch công khai nào xảy ra. Bằng cách đó, các cá nhân trao đổi tài sản với nhau chỉ phải công bố giao dịch của mình cho mọi người thấy. Những người đang giữ bản sao luận án sẽ xác minh (validate) các giao dịch đó, và nếu hợp lệ, sẽ ghi giao dịch hợp lệ (validated transcaction) vào sổ cái mình đang giữ. Một sổ cái phi tập trung như thế đảm bảo 3 tính chất sau cho mọi giao dịch công khai:

(•) Minh bạch: mọi giao dịch được thực hiện công khai với các nhân chứng là những cá nhân đạng giữ sổ cái.

(•) Toàn vẹn: không ai có thể sửa đổi nội dung của giao dịch đã được ghi xuống vì không thể thông đồng được với mọi người giữ sổ cái.

(•) An toàn: sổ cái không bị phá hủy (nếu còn lại một vài người đang giữ sổ cái).

Công nghệ hiện thực hóa khái niệm sổ cái thỏa 3 tính chất trên gọi là **công-nghệ-sổ-cái-phi-tập-trung**.

**XÂU CHUỖI – MỘT CÀI ĐẶT CHO SỔ CÁI PHI TẬP TRUNG**

**Xâu khối và sổ cái phi tập trung**

Xâu khối – **Blockchain** viết liền, như tên gợi ý, là tập các khối (*block*) được kết lại (*chain*) với nhau xích tạo thành một sợi xích với các mắt xích là các khối (blockchain):…

Hai thành phần chính làm nên blockchain là:

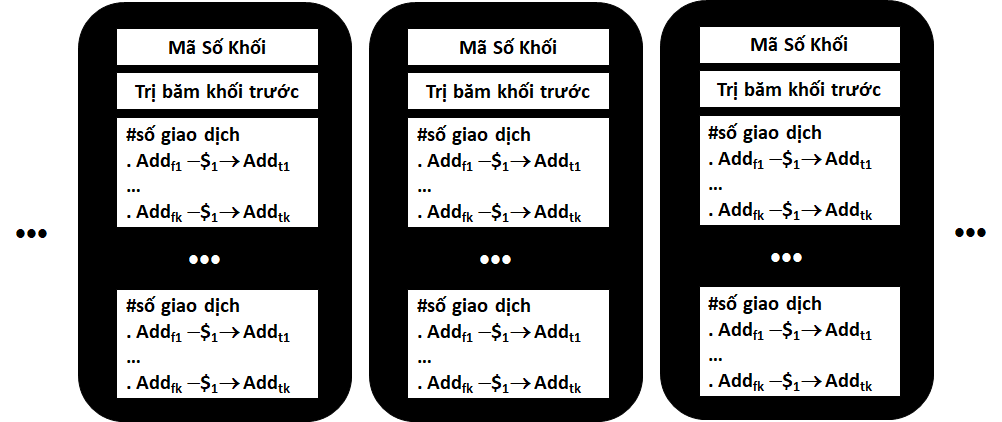
(**1**) **block**: tựa như một trang (*page*) của sổ cái (*ledger*) với nội dung là tất cả các giao dịch (*transactions*) được ghi lên trang đó. Ta sẽ gọi là khối hàm ý tính vững chắc của trang theo nghĩa không thể hị hư hại những thứ đã ghi trên đó.

(**2**) **chain**: tựa như một mắt xích (*chain*) kết chặt một khối mới với khối trước đó. Các khối chỉ được thêm vào cuối chuỗi và chuỗi dài dần ra.

**Xâu khối và công nghệ thông tin**

Trong khoa học máy tính, khái niệm xâu khối – blockchain[[2]](#footnote-2) hoàn toàn có thể được cài đặt bằng một cấu trúc dữ liệu đặc biệt kiểu danh sách liên kết (*list*) trong đó mỗi khối là một trang (*page*) các bản ghi (*record*) lưu trữ thông tin của một giao dịch (*transaction*)[[3]](#footnote-3), và một số thông tin quan lý khác.

**Blockchain** là **list** (*danh sách*) đặc biệt ở chỗ với **list**, để liên kết thì khối sau giữ địa chỉ (*address*) của khối trước (trong nhiều ngôn ngữ liên kết này được thể hiện qua kiểu con trỏ (pointer)); nhưng trong **blockchain**, khối sau giữ mã-chứng-thực (**MAC** – *Message Authentication Code*) của khối trước (chính là trị băm mật mã (*cryptographic-hash value*) của thông điệp (message) là toàn bộ nội dung của khối trước.).



Như vậy, blockchain gần với khái niệm tập hợp (*set*) hơn là khái niệm mảng (*array*) hay danh sách liên kết (*list*) theo nghĩa phải duyệt tuần tự (sequence search) để tìm block hay Tx cần tìm. Điều này phù hợp với lưu trữ dạng tập tin (*file*) trên thiết bị phần cứng.

**Xâu khối và khoa học máy tính**

Bên cạnh việc tổ chức sổ cái như xâu các khối (*chain of blocks: blockchain*), mỗi khối là bản ghi (*record*) chứa tập hợp các giao dịch (*Tx*), và được lưu trên thiết bị phần cứng như một CSDL phi tập trung (*decentralized database*), theo nghĩa CSDL được lưu trữ trên nhiều máy một cách độc lập với nhau nhưng vẫn đảm bảo tính nhất quán của CSDL chung. Như vậy, để duy trì sổ cái cần (**i**) một hạ tầng kiến trúc mạng và các thuật toán truyền thông mạng hiệu quả và (**ii**) các thuật toán đồng bộ dữ liệu giữa các CSDL được lưu trữ trên các điểm khác nhau.

***Hạ tầng mạng cho blockchain***

Vấn đề truyền thông mạng được giải quyết và hiện thực trên kiến trúc mạng ngang hàng (**P2P network** – *peer-to-peer network*), ở đó các nút mạng liên kết vào trao đổi thông tin trực tiếp, không qua trung gian. Các nút mạng được trang bị các thuật toán để quét mạng liên tục và sẵn sàng cập nhật CSDL khi có một block mới xuất hiện.

***Đồng bộ dữ liệu***

Tính nhất quán của CSDL chung được đảm bảo qua các thuật toán được biết với tên thuật-giải-đồng-thuận (*consensus algorithm*) mà được xây dựng dựa trên nguyên tắc đồng-thuận-số-đông, theo đó, block mới sẽ được thêm vào chain dài nhất hiện tại.

Một cách tổng quát, blockchain là một CSDL phi-tập trung (decentralized database).

**CÔNG NGHỆ CHUỖI KHỐI**

Công nghệ chuỗi khối (*blockchain technology*) là một nền tảng (*platform*) cung cấp các cơ chế cũng như công cụ cho phép hình thành và duy trì một mạng chuỗi khối (*blockchain network*).

**Mạng chuỗi khối**

Mạng chuỗi khối hình thành từ các nút (*node*) mạng hoạt động độc lập, giao tiếp với các nút khác theo giao thức mạng ngang hành. Mỗi nút tham gia mạng chuỗi khối với một định danh (*identification*) duy nhất và cũng chính là tài khoản của người sở hữu nút đó, vì thế, nhìn dưới góc nhìn tài chánh-ngân hàng, định danh này chính là số tài khoản (*account number*) của ngươi đó.

Có 2 loại nút trong mạng chuỗi khối là nút sử dụng (*user node*) và nút duy trì (*miner node*) dữ liệu của CSDL blockchain.

***Nút sử dụng dữ liệu chuỗi khối – user node***

Là bất kỳ thiết bị nào có thể kết nối mạng để thực hiện các giao dịch liên quan đến thông tin được lưu giữ trong CSDL blockchain. Để giao dịch các dữ liệu của riêng mình, user node phải có khóa sử dụng tài khoản, như mã nhận dạng cá nhân (*Pin Code – Personal Identification Number*) được dùng để sử dụng thẻ ATM của ngân hàng. Khóa sử dụng tài khoản và số tài khoản có một quan hệ toán học chặt chẽ. Thực chất chúng là cặp khóa gốm khóa cá nhân (*private key*) và khóa công khai (*public key*) của một hệ mã công khai hiện đại (advanced public key cryptosystem), và địa chỉ (*address*) được phái sinh từ khóa công khai (nhiều mạng chuỗi khối, còn cho phép sử dụng trực tiếp khóa công khai làm địa chỉ tài khoản).

***Nút duy trì mạng chuỗi khối – miner nodes***

Là những máy chủ (*server*) đủ mạnh để có thể lưu giữ toàn bộ CSDL chuỗi khối, từ khối đầu tiên đến khối mới nhất và còn tiếp tục cập nhật thêm các khối tiếp nữa. Do tính chất bất biến của dữ liệu lưu trữ trong mạng chuỗi khối, các khối chỉ được thêm vào chuỗi chứ không thể xóa hay sủa đổi. Hơn nữa, chỉ các khối hợp lệ (*validated block*) mới được gắn thêm (*chain*) vào chuỗi. Một Các miner nodes có nhiệm vụ kiểm tra (*verify*) các giao dịch hợp lệ tập hợp trong khối hợp lệ và tranh đua cùng các miner nodes khác trong một trò chơi (*game*) được thiết kế riêng cho từng chuỗi khối để trở thành nút tạo được khối mới nhanh nhất. Khối mới này sẽ được gắn vào chuỗi khối và cuộc đua tạo khối mới lại tiếp tục.

Miner node cũng có thể có thông tin riêng của nó. Nghĩa là miner node hàm ý cũng là user node khi tham gia các giao dịch trao đổi thông tin của nó với các nút mạng khác trong cùng một mạng chuỗi khối.

**Các công nghệ cốt lõi của chuỗi khối**

Như ta đã thấy, chuỗi khối thực chất là một CSDL phi-tập trung được lưu trữ trên nhiều nút mạng trong mạng chuỗi khối (*blockchain network*). CSDL này chỉ được phép gắn thêm vào, mọi thao tác có thể làm thay đổi dữ liệu đã lưu như sửa đổi (*edit*) hay xóa (*delete*) đều không được phép. Nguyên do là khi một miner node thay đổi dữ liệu nó đã lưu đồng nghĩa nó tự loại mình ra khỏi mạng các nút duy trì chuỗi khối và chỉ có thể là nút sử dụng.

Dữ liệu trong CSDL chuỗi khối phải đảm bảo tính toàn vẹn (*integrity*).

Tính toàn vẹn của dữ liệu trong CSDL chuỗi khối được đảm bảo bởi công nghệ mật mã hiện đại bao gồm mã chứng thực thông điệp- và khóa sử dụng thông tin tài khoản.

Mọi dữ liệu được băm bằng một hàm băm mật mã (*cryptographic hash function*) và được ký (*sign*) bằng khóa cá nhân của người tạo ra dữ liệu đó.

CSDL chuỗi khối chỉ cho phép xem (*view*) và thêm các khối hợp lệ vào.

Một khối hợp lệ tạo là khối được bởi một miner node chiên thắng (*winner*) trong một trò chơi (*game*) được thiết kế riêng cho từng mạng chuỗi khối.

Như vậy, 3 lý thuyết cũng như công nghệ nền tảng làm trụ cột cho chuỗi khối gồm: lý thuyết trò chơi – mật mã hiện đại – mạng ngang hàng.

***Lý thuyết trò chơi***

Lý thuyết trò chơi là khoa học nghiên cứu các mô hình toán học về tương tác chiến lược giữa các tác nhân. Lý thuyết trò chơi có ứng dụng trong mọi lĩnh vực khoa học xã hội, cũng như logic, khoa học hệ thống và khoa học máy tính. Các khái niệm về lý thuyết trò chơi cũng được sử dụng rộng rãi trong kinh tế học. Lý thuyết trò chơi tiên tiến được áp dụng cho nhiều mối quan hệ hành vi và hiện tại được xem như một thuật ngữ chung cho khoa học về việc ra quyết định hợp lý ở con người, động vật cũng như máy tính.

Lý thuyết trò chơi được phát triển rộng rãi vào những năm 1950 và đã được áp dụng cho các quá trình tiến hóa vào những năm 1970, mặc dù những khái niệm tương tự đã có từ những năm 1930. Lý thuyết trò chơi đã được thừa nhận rộng rãi như một công cụ quan trọng trong nhiều lĩnh vực.

Tài liệu này không nghiên cứu nhiều về lý thuyết trò chơi cũng như công nghệ mạng ngang hàng mà tập trung chủ yếu vào công nghệ mật mã hiện đại.

***Mạng ngang hàng***

Mạng ngang hang (**P2P**) là mạng các máy tính trong đó hai hoặc nhiều máy tính có thể chia thông tin mà không yêu cầu máy chủ hoặc phần mềm máy chủ riêng biệt.

Ở dạng đơn giản nhất, mạng **P2P** được tạo ra khi hai hay nhiều máy tính được kết nối và chia thông tin mà không cần thông qua một máy chủ riêng. Mạng **P2P** có thể là một kết nối đặc biệt — một số máy tính được kết nối qua Universal Serial Bus để truyền tập tin (*file*). Mạng **P2P** cũng có thể là một cơ sở hạ tầng cố định liên kết nhiều máy tính trong một văn phòng nhỏ qua dây cáp. Hoặc mạng **P2P** có thể là mạng ở quy mô lớn, trong đó các giao thức và các ứng dụng đặc biệt thiết lập mối quan hệ trực tiếp giữa những người dùng qua Internet.

Việc sử dụng mạng **P2P** ban đầu trong kinh doanh diễn ra sau khi triển khai các máy tính cá nhân độc lập vào đầu những năm 1980. Các máy tính cá nhân lúc bấy giờ có ổ cứng độc lập và CPU tích hợp. Các thiết bị mạng thông minh cũng có các ứng dụng tích hợp, nghĩa là chúng có thể được triển khai trên máy tính để bàn và hữu ích mà không cần dây nối chúng với máy tính lớn.

Cũng như lý thuyết trò chơi như lưu ý trên, tài liệu này không tập trung nhiều vào công nghệ mạng **P2P** mà sử dụng các giao thức tổng quát của mạng **P2P** cho mục đích chia sẻ thống tin.

***Mật mã hiện đại***

Mật mã học là kỹ thuật bảo mật thông tin và liên lạc thông qua việc sử dụng mã để chỉ những người có quyền sử dụng thông tin mới có thể hiểu và xử lý nó. Do đó ngăn chặn truy cập trái phép vào thông tin. **Crypt**o**graph**y được cấu thành từ tiền tố “*crypt*” có nghĩa là “*ẩn*” và hậu tố “*graph*” có nghĩa là “*viết*” – viết ẩn (nghĩa). Các kỹ thuật được sử dụng để bảo vệ thông tin được khai thác từ các khái niệm toán học và tập các phép tính theo thuật toán (*algorithm*) để chuyển đổi thông điệp (*message*) theo những cách khiến việc giải mã nó trở nên khó khăn. Các thuật toán này được sử dụng để tạo khóa mã hóa (*encryption key*), chữ ký số (*digital signature*), xác minh (*authentication*) để bảo vệ quyền riêng tư của dữ liệu (*data privacy*), và để bảo vệ các giao dịch bí mật như giao dịch thẻ tín dụng và thẻ ghi nợ.

Quá trình chuyển đổi một văn bản rõ (*plain text*) thành văn bản mật mã (*cipher text*), là văn bản được tạo ra sao cho chỉ người nhận văn bản hợp pháp có thể giải mã nó, được gọi là mã hóa (*encryption*). Quá trình chuyển đổi văn bản mã (*cipher text*) thành văn bản rõ (*plain text*) được gọi là giải mã (*decryption*).

Các hệ mã hiện đại (*advanced cryptosystem*) có các đặc tính sau:

**Tính bảo mật**: Thông tin chỉ có thể được truy cập bởi người hợp pháp và không người nào khác có thể truy cập thông tin mật này.

**Tính toàn vẹn**: Thông tin không thể được sửa đổi trong quá trình lưu trữ hoặc chuyển tiếp giữa người gửi và người nhận hợp pháp mà không phát sinh thông tin bổ sung.

**Chống từ chối**: Người tạo/người gửi thông tin không thể phủ nhận thông tin của mình đã gửi.

**Xác thực**: Danh tính của người gửi và người nhận được xác nhận. Cũng như điểm đến/nguồn gốc của thông tin được xác nhận.

Nói chung có ba loại mật mã: mã đối xứng (*symmetric cryptosystem*), hàm băm mật mã hay gọi tắt là hàm băm (*hash function*), và mã bất đối xứng (*asymmetric cryptosystem*).

**Mật mã khóa đối xứng**: Là một hệ thống mã hóa trong đó người gửi và người nhận sử dụng một khóa chung duy nhất (*pre-share key/secrete key/key*) để mã hóa và giải mã thông điệp. Mã đối xứng nhanh và đơn giản nhưng vấn đề nằm ở chỗ làm sao thiết lập khóa chung một cách an toàn giữa người gửi và người nhận. Hệ mật mã khóa đối xứng phổ biến nhất là hệ mã hóa dữ liệu (DES – *Data Encryption System*) và hệ mã hóa nâng cao (AES – Advanced Encryption System).

**Hàm băm**: Không sử dụng khóa trong thuật toán này. Trị băm có độ dài cố định được xác định theo văn bản khiến nội dung của văn bản không thể phục hồi. Nhiều hệ điều hành sử dụng hàm băm để mã hóa mật khẩu. Các hàm băm phổ biến là MD5 (*Message Digest 5*) thường được dùng bảo mật mật khẩu trong các hệ thống thông tin; và SHA-2 (*Secure Hash Algorithm 2*) hiện được các mạng chuỗi khối sử dụng.

**Mật mã khóa bất đối xứng**: Trong hệ thống này, một cặp khóa được sử dụng để mã hóa và giải mã thông tin. Khóa công khai (*public key*) của người nhận được người gửi sử dụng để mã hóa và khóa cá nhân (*private key*) của người nhận được sử dụng để giải mã. Khóa công khai và khóa cá nhân phải khác nhau và có quan hệ toán học chặt chẽ. Ngay cả khi khóa công khai có thể được công bố cho mọi người được biết thì chỉ người nhận có khóa cá nhân tương ứng mới có thể giải mã. Thuật toán mã hóa khóa bất đối xứng phổ biến nhất là thuật toán RSA. Hiện tại, hệ mã dưa trên đường cong elliptic (ECC – Elliptic Curve Cryptogsystem) đang được sử dụng trong các mạng chuỗi khối do tính hiệu quả và an toàn của nó.

1. ERM do Peter Chen đề xuất năm 1976 (The Entity-Relationship Model: Toward an Unified View of Data, MIT, 1976) [↑](#footnote-ref-1)
2. Trong tài liệu này, thuật ngữ blockchain sẽ được sử dụng thay cho từ Việt hóa xâu-khối. [↑](#footnote-ref-2)
3. Trong tài liệu này, từ Tx sẽ được dùng để khí hiệu cho giao dịch – transaction. [↑](#footnote-ref-3)